October 2024

HIPAA Privacy Training

HCP Provider Compliance Training Module

HealthCare Partners, IPA
HealthCare Partners, MSO

Key Topics

Welcome to HealthCare Partners HIPAA Privacy Training! By completing this course, you will become knowledgeable about the following key topics as a HCP provider:

- ✓ What is HIPAA?
- ✓ HITECH Act
- ✓ Who is Affected by HIPAA?
- ✓ HIPAA Privacy & Security
- ✓ Protected Health Information (PHI)
- ✓ De-identification of PHI
- ✓ What is not Considered PHI?
- ✓ Covered Entities
- ✓ Business Associates
- ✓ Patient Rights under HIPAA
- ✓ Permitted Uses & Disclosures of PHI
- ✓ Authorizations for Disclosures
- ✓ Breach Notification Rule
- ✓ Privacy & Security Best Practices
- ✓ Your Role

Provider & FDR Compliance Training Requirement

Following this training,
you must also submit the online Provider & FDR Compliance Attestation to be in compliance with this requirement.

To Access the Training Attestation Form:

1. Scroll down to the Provider & FDR Compliance Attestation section, just below the training modules found on the HCP Compliance Program webpage at www.HealthCarePartnersNY.com.

2. Click on Online Attestation Form to complete.

3. Click Save and Submit.

What is HIPAA?

Health **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996

The Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information.

HealthCare Partners (HCP) Workforce members and providers receive and manage health information about our members. It is important to protect the privacy of this health information and other confidential information with which we come into contact.

What is HIPAA? (Cont'd.)

HIPAA was enacted to achieve the following goals:

- ✓ <u>Health Care Reform</u>
  - Continued health insurance coverage for individuals who lose or change jobs ("Portability")
  - Established national standards for electronic data transmission (e.g., enrollment, eligibility, claims, and payment transactions)
  - More efficient, simpler, and less costly health care system
- ✓ <u>Privacy and Security of Health Information</u>
  - Sets minimum standards to protect the integrity, availability, and confidentiality of patient information ("Accountability")
  - Defines penalties for violations

HITECH ACT

Health **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth **A**ct of 2009

The HITECH Act was enacted under the American Recovery and Investment Act of 2009, resulting in significant changes to HIPAA Privacy and Security, including:

- widening the scope of privacy and security protections;
- increasing the potential legal liability for non-compliance; and
- providing more enforcement.

The Act also created incentives among providers to use health care information technology, such as electronic health record (EHR) systems.

HIPAA Privacy & Security

Privacy

Privacy refers to the protection of a member's health care data and defines which data is to be protected, including how member data is used and disclosed.

Security

Security refers to the systems in place to guard the integrity of and accessibility of protected health information in electronic form. Security protects data integrity, confidentiality, and availability by using administrative, physical, and technical safeguards.

HIPAA Privacy & Security (Cont'd.)

HIPAA Privacy Rule	
What does the rule do? • Established standards to protect all forms (written, verbal, or electronic) of information created or received by health care providers, employers, health plans or other "Covered Entities". • Gives patients certain rights and control over their health information.	**Examples of protected information:** Individually identifiable information such as: • Name and address • Phone number • Social Security number • Health care specifics • Payment information Information pertaining to HIV, alcohol or substance abuse, mental health and genetics requires additional protections.

HIPAA Privacy & Security (Cont'd.)

HIPAA Security Rule	
What does the rule do? • Established to safeguard electronic protected health information (ePHI)* • Outlines security procedures to ensure the confidentiality, integrity and availability of protected health information (PHI) *ePHI is protected health information stored on computers, storage devices, or in any electronic system.	How is health information protected? As required by the Security Rule, the appropriate administrative, physical, and technical safeguards must be used to protect ePHI.

See the next slide for examples of administrative, physical and technical safeguards.

HIPAA Privacy & Security (Cont'd.)

Administrative Safeguards

Security Official & Personnel

Policies & Procedures

Risk Assessment & Management Process

Physical Safeguards

Facility Access Controls

Workstation & Device Security

Technical Safeguards

System Access Controls

Audit Controls

Electronic Data Transmission Security

Who is Affected by HIPAA?

- Employees who handle, use, or know individuals' Protected Health Information (PHI)
- Health care providers (health departments, hospitals, doctors' offices, any agency that transmits PHI electronically)
- Health plans that provide or pay the cost of medical care (e.g., Medicaid, Medicare, CHAMPUS, BC/BS, HMOs)
- Trading Partners – electronically exchange PHI
- Business Associates – perform services on your behalf
- HIPAA also applies to you as a consumer of healthcare!

Confidentiality

Confidentiality applies to all types of information including information pertaining to:

- Patients
- Employees
- Social Security numbers
- Credit card numbers and other financial data
- System IDs and passwords
- Company data and processes

Confidential information should only be accessed, used or shared when necessary to carry out your responsibilities related to member care.

Protected Health Information

Protected Health Information or “PHI” refers to ***individually identifiable health information in any form*** or medium (e.g., verbal, paper, electronic) that is **transmitted or stored** and **that can be linked to a specific individual by a *unique identifier***.

When personally identifiable information (PII) is used in conjunction with information about a person’s physical or mental health condition, health care, or payment for that health care, it becomes PHI.

Examples of PHI can be found in:

- Medical and billing records
- Insurance/benefit enrollment and payment information
- Claims adjudication documentation
- Case or medical management records

Member health information in any form is considered PHI.

Protected Health Information (Cont'd.)

Under HIPAA, the following **18 unique identifiers** are considered personally identifiable information. This information can be used on its own or with other sources to identify, contact, or locate an individual.

Name	Account number
Address (all geographic subdivisions; including street, city, county state and zip code)	Certificate or license number
All elements of dates (including date of birth or death, admisssion and discharge dates)	VIN (Vehicle ID Number)
Telephone number	Device identifier/serial number
Fax number	Web URL
Email address	Internet Protocol (IP) address
Social Security Number	Biometric identifiers (voice or finger print)
Medical record number	Photographic image
Health plan beneficiary number	Any other characteristic that could identify an individual

De-identified PHI

If a communication contains any of the unique identifiers, or parts of the identifier, such as initials, the data is considered “identified”.

To be considered “de-identified”, **ALL** of the 18 HIPAA Identifiers must be removed from the data set so that the information cannot be linked to an individual.

For research, marketing and fundraising purposes, **ALL** PHI must be de-identified.

De-identified information is not considered PHI and therefore, is not protected under the HIPAA Privacy Rule.

What is NOT considered PHI?

Not all PII is considered PHI. HIPAA does NOT consider the following data to be PHI:

Education Records: Health information contained in education records (e.g., student medical records).
Employment Records: held by a covered entity in its role as an employer (e.g., medical history of an HCP employee in their personnel file).
Non-PII: Health data that is not shared with a covered entity or is not personally identifiable (e.g., blood pressure records that do not contain PII).

Preemption of state law:

The HIPAA Privacy Rule overrides any other state law unless that state law provides more protection for the member.

Covered Entities

All covered entities and business associates who use, store, maintain, transmit or dispose of patient health information (in any form) must follow HIPAA Privacy and Security standards.

HIPAA Covered Entities include:

Health Care Plans or Insurers

- Health insurance companies
- HMOs
- Employer sponsored group health plans

Health Care Clearinghouses

Entities that process non-standardized information they receive from an entity into a standard format (e.g., billing companies processing electronic claims data).

Certain Health Care Providers

- Doctors, nurses, dentists, & psychologists
- Hospitals & clinics
- Nursing homes
- Labs
- Pharmacies

Business Associates

Who are Business Associates?

A Business Associate is an individual or entity, other than a member of a Covered Entity's workforce, who performs functions on behalf of, or provides certain services to, a Covered Entity that involve access to PHI.

EXAMPLES	EXCEPTIONS
Claims processing/medical billing companies	A HCP employee
Medical transcription companies	Healthcare providers, if the disclosure of PHI by another Covered Entity is related to the individual's healthcare treatment
Answering services	Financial institutions when performing only payment processing activities
Document storage or disposal (shredding) companies	Janitorial service companies, maintenance & repair personnel
Health information exchanges	Conduits of PHI, (e.g., U.S. postal service, messenger services)

Business Associates (Cont'd.)

Business Associate Agreements

A Business Associate Agreement or BAA is a required special contract between a Covered Entity and a Business Associate. The BAA:

- ✓ outlines the permitted uses and disclosure of PHI;
- ✓ describes appropriate privacy and security standards and safeguards;
- ✓ contractually obligates the Business Associate to maintain those standards; and
- ✓ subjects the Business Associate to civil and criminal penalties for HIPAA violations.

HCP as a Covered Entity, has a BAA with each of our Business Associates.

If you think one of our Business Associates is not respecting our members' privacy, you must report your concern by calling our **Compliance Hotline at (888) 475-8376** or submitting an online report via **hcphotline.ethicspoint.com**.

Patient Rights Under HIPAA

HIPAA privacy standards also outline patient rights regarding their PHI. These rights give our members control over how HCP and our Business Associates use and disclose their PHI.

HCP members have the right to:

(1) Receive a Notice of Privacy Practices (NOPP) – The NOPP must be provided by the member's provider or health plan. The NOPP must be in plain language and presented to members at the time of their first visit or assessment for eligibility.

The NOPP must inform members of the following:

- how their information will be used or shared
- their rights to access their own information
- their right to receive confidential communications
- how to file a complaint
- the Privacy Officer's contact information

Patient Rights Under HIPAA (Cont'd.)

(2) Request amendments to their medical record – Members may request a change, edit or update to their medical record in the form of an amendment if he/she believes it is incomplete or incorrect.

(3) Access, inspect and obtain copies of their medical record – Members can request* to view and obtain copies (paper or electronic) of their medical records at any time. The medical record must be provided in the form and format requested. That includes inspecting their records in person and taking notes or photographs of their PHI.

* Requests for access may be made orally or in writing. You must take reasonable steps to verify the individual's identity).

DESIGNATED RECORD SET

As indicated above, members may access, upon request, their health information about them in one or more designated record sets, including medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used to help make a decision about the individual.

Patient Rights Under HIPAA (Cont'd.)

(4) Request restrictions on certain disclosures if other than for treatment, payment or health care operations (TPO). Members can also request restrictions on disclosures to health plans concerning treatment for which the member paid out of pocket. We are not required to agree with the requested restrictions.

(5) Receive an accounting of non-routine disclosures when their PHI is shared with an outside party for reasons other than for TPO. The report should include the dates, recipient name(s), specific information disclosed, and the reason for the disclosure.

(6) Confidential Communications – Members may request to receive communications about their PHI through alternative means (e.g., via secure text message) or to an alternate address.

Patient Rights Under HIPAA (Cont'd.)

(7) File a complaint of a privacy violation – Members have the right to file a complaint directly with HCP or to the Office for Civil Rights (OCR) if he/she believes their HIPAA privacy rights have been violated. HCP and its' providers are required to provide contact information for filing a complaint.

To stay updated on changes to the HIPAA Right of Access Initiative go to: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Permitted Uses & Disclosures of PHI

General Rule

An entity may not use or disclose PHI, except as permitted or required by the Privacy Rule, such as to an individual when requested and to HHS to investigate or determine compliance with the Privacy Rule, or when otherwise required by law.

Disclosure of PHI is required by law for the following circumstances:

Public health	Cadaveric organ, eye, or tissue donations
Victims of abuse, neglect or domestic violence	Research purposes
Health oversight activities	Aversion of serious health threat or safety
Judicial or administrative proceedings	Specialized government functions
Law enforcement purposes	Workers' compensation
Coroners, medical examiners, and funeral directors about descendants	

Authorization for Disclosures

Members PHI should not be used for reasons other than treatment, payment, or health care operations (TPO), unless we get a written authorization.

An authorization must be specific to the particular situation for which it is being requested, and it has a limited duration.

Exception: a provider can release a child's immunization record without a HIPAA authorization if required by state law for admission.

Minimum Necessary Rule

PHI that is accessed, used or shared for purposes other than for TPO should be limited to the *minimum necessary* information needed to accomplish your job.

Enforcement & Penalties

The Office for Civil Rights (OCR) enforces both civil and criminal mandatory penalties for HIPAA/HITECH violations. Penalties are enforced based on knowledge and intent.

As of 1/15/2024

- **Civil Penalties =** $141 to $71,162 per violation; Max of $2.1mil per year for the same violation
- **Criminal Penalties =** $50,000 to $250,000 per violation + up to 10 years in prison)

Type of Violation (Based on Degree of Fault)	**HIPAA Penalty (Based on Nature, Extent of Violation & Potential Harm)**
Tier 1: Lack of knowledge =	$137 - $68,928 per violation
Tier 2: Reasonable cause =	$1,379 - $68,928 per violation
Tier 3: Willful neglect, but issue corrected within 30 days =	$13,785 - $68,928 per violation
Tier 4: Willful neglect + failure to correct w/in 30 days =	$68,928 - $2,067,813 per violation

Breach Notification Rule

The Breach Notification Rule requires covered entities and their business associates to notify patients when their unsecured PHI is impermissibly acquired, accessed, used or disclosed (or “breached”) in a way that compromises the privacy and security of the PHI or ePHI.

What are some breach exceptions?

(1) **Unintentional acquisition, access or use of PHI** by a staff member in good faith within the scope of their authority, when the PHI is not further disclosed;

(2) **Inadvertent disclosure** of PHI from one authorized person to another authorized person at HCP, when the PHI is not further disclosed; and

(3) When the individual/ or entity disclosing the PHI believes in good faith the unintended recipient of the PHI has the **inability to retain the PHI**.

Breach Notification Rule – Cont'd.

What is considered a reportable breach under HIPAA?

A breach is considered reportable if the covered entity or business associate cannot demonstrate that there is a low probability that the data that was improperly accessed, used or disclosed has been compromised based on a risk assessment.

Reporting Requirements

1) **Notifying individuals:** Covered entities must notify individuals affected by a breach.

2) **Notifying the media:** If a breach affects 500 or more residents of a state or jurisdiction, covered entities must notify major media outlets in that area.

3) **Notifying the Secretary of Health and Human Services (HHS):** Covered entities must notify HHS electronically if a breach occurs, within 60 calendar days of the discovery of the breach.

Privacy & Security Best Practices

ALWAYS

- ✓ Log off before you walk away from your computer
- ✓ Verify fax numbers & email addresses before sending PHI
- ✓ Verify the identity of the caller before releasing confidential information
- ✓ Discuss patient information in private locations
- ✓ Access information on a need-to-know basis, only to do your job
- ✓ Share only the minimum information necessary for the intended purpose of the disclosure
- ✓ Dispose of confidential information properly (e.g., locked shredder bins)
- ✓ Use only secure and approved email methods or Internet connections when sending or accessing PHI

NEVER

- **X** Never share your password with anyone
- **X** Leave PHI unattended or visible on your desktop or computer screen

Privacy & Security Best Practices (Cont'd.)

HIPAA Compliance for a Doctor's Office

Exercise privacy **EVERYWHERE** in your office.

PROMINENTLY DISPLAY the Notice of Privacy Practices in your office and on your website.

EXERCISE CAUTION when using and disclosing PHI.

Conduct a mandatory annual **RISK ASSESSMENT**.

Maintain and follow security & privacy **POLICIES & PROCEDURES**.

Conduct **HIPAA TRAININING** for your staff & physicians annually.

Your Role

Remember that health information ultimately belongs to the patient, not to their provider or their health plan. Just as you expect your health care information to be kept private, so do the patients.

Your commitment to patient care includes a commitment to respecting your patients privacy.

HealthCare Partners, IPA
HealthCare Partners, MSO